**King County**
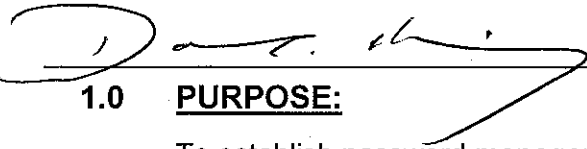
**Office of Information
Resource Management**

# Information Technology Governance Policies and Standards

| Title | Document Code No. |
|---|---|
| **Password Management Policy** | ITG-POS-02-02 |

| Chief Information Officer Approval | Date | Effective Date. |
|---|---|---|
| *[signature]* | | 9/9/09 |

## 1.0 PURPOSE:

To establish password management practices which ensure the appropriate protection of King County information assets and maintain accountability.

## 2.0 APPLICABILITY:

This policy is applicable to all King County information assets, including applications and systems, Organizations and Workforce Members.

## 3.0 REFERENCES:

3.1 Enterprise Information Security Policy

3.2 Information Technology Policy and Standards Exception Request Process

## 4.0 DEFINITIONS:

4.1 **Active Directory**: A directory service from Microsoft Corporation that serves as the central authority for network security, providing Workforce Member Authentication and access control to network resources.

4.2 **Administrative Resource:** Such as routers, switches, WAN links, firewalls, servers, Internet connections, administrative-level network operating System Accounts, Active Directory and Directory Enterprise Administrative level accounts and any other IT resource.

4.3 **Authentication:** A security procedure designed to verify that the authorization credentials entered by a Workforce Member to gain access to a network or System are valid.

4.4 **Automated Logon Process:** Storing Authentication Credentials in a registry entry, macro, or function to automatically authenticate a User to a System without User intervention.

4.5 **Information Asset:** A definable piece of information, information processing equipment, or information system, that is recognized as "valuable" to the Organization that has one or more of the following characteristics:
- Not easily replaced without cost, skill, time, resources, or a combination thereof

- Part of the Organization's identity, without which, the Organization may be threatened

4.6 **Organization**: Every county office, every officer, every institution, and every department, division, board and commission.

4.7 **Passphrase:** An exceptionally long password generally derived from a phrase or short sentence that typically eliminates spaces and replaces some letters with special characters; for example "TheDark3stHourI$JustBeforeDawn". (Do not use this example.)

4.8 **System**: Software, hardware and interface components that work together to perform a set of business functions.

4.9 **System Account**: A specialized Workforce Member account, generally used by an operating System to start a process for an application. Accounts of this type typically have elevated privileges on the specific System running the application for which they are used.

4.10 **Two-Factor Authentication:** A security process that confirms User identities using two distinctive factors – something they have and something they know. Risk of fraud is reduced by requiring two different forms of electronic identification.

4.11 **Workforce Members**: Employees, volunteers, and other persons whose conduct, in the performance of work for King County, is under the direct control of King County, whether or not they are paid by King County. This includes full- and part-time elected or appointed officials, members of boards and commissions, employees, affiliates, associates, students, volunteers, and staff from third-party entities who provide service to King County.

## 5.0 POLICIES:

5.1 **Mandatory Use** – Workforce Members must use appropriate authentication credentials consisting of at least a login-ID and password to validate their identity when connecting to King County Information Assets. Each workforce member must be issued unique authentication credentials.

5.2 **Storing Passwords** – Organizations shall require that any Authentication System that stores passwords must store them in an encrypted format. When developing and/or acquiring Systems or Application Software Organizations shall not consider any solution that requires the storage of passwords within the system in an unencrypted format.

5.3 **Accountability** – Workforce Members are accountable for all activities performed under their Authentication Credentials unless an investigation proves that the Workforce Member did not violate this policy at the time of the incident requiring the investigation.

5.3.1 **Vendor Default Authentication Credentials:** To ensure accountability and security all newly installed systems will have vendor default authentication credentials changed, disabled or removed.

# Password Management Policy

### 5.4 Password Management

#### 5.4.1 Password Issuance

5.4.1.1 **Identity Authentication** - Organizations shall implement a procedure to authenticate the identity of the Workforce Member receiving a new or changed password.

5.4.1.2 **Forced Change** - Organizations shall implement a System procedure that forces the Workforce Member to choose a password before the logon process is complete when the password is issued by a System Administrator.

#### 5.4.2 Sharing Passwords – Workforce Members shall keep their password secret and shall not make their password known to anyone else, including management, supervisors, personal assistants, human resources and System Administrators. Workforce Member passwords must not be shared under any circumstance.

#### 5.4.3 Displaying Passwords - Organization shall implement Systems that mask, suppress, or otherwise obscure the display of passwords, so unauthorized parties cannot observe or subsequently recover them.

#### 5.4.4 Changing Passwords – Whenever possible Organizations shall implement System password Policies that automatically force the Workforce Member to change their password at least every ninety (90) days. When automation is not possible, Workforce Members must manually change their passwords at least every ninety (90) days. Workforce Members must also change their password immediately after their password or an Information Asset that they access using their password has been, or is suspected of being compromised.

#### 5.4.5 Password History – Whenever Possible Organizations shall implement a system which prohibits the re-use of at least, the last four passwords.

#### 5.4.6 Failed Login Attempts – When the technology allows, Organizations shall implement a process that after five (5) unsuccessful attempts to enter a password the user account is disabled for at least thirty (30) minutes unless unlocked by the System Administrator.

#### 5.4.7 Automated Logon - Workforce Members shall not use passwords in any Automated Logon Process.

#### 5.4.8 Password Composition – Workforce Members shall use strong passwords and Organizations shall implement password Policies that require Workforce Members to choose strong passwords that are:

5.4.8.1 **Length** - At least eight (8) characters in length or the maximum length permitted by the System, whichever is shorter.

5.4.8.2 **Elements** - Contain at least three (3) of the following four (4) elements:
- English upper case letters:     A, B, C...Z
- English lower case letters:     a, b, c...z
- Westernized Arabic numbers:     0, 1, 2...9

- Special characters:      { } . ' \ ` ! @ # $ % ^ & ( ) - (Windows)

@ # $ (Unix, Linux, mainframe)

5.4.9 **Passwords Containing Identifying Characteristics** – Organizations shall not assign passwords that contain personal information, including but not limited to name (or part of a name) birth date, social security number (or any part of the social security number) driver's license number, or employee number.

### 5.5 Administrative and/or System Account Password Management

#### 5.5.1 Limit Password Access

5.5.1.1 **Need to Know** - Organizations shall limit access to administrative and System passwords to System Administrators who have a need to know.

5.5.1.2 **Store Securely** - System Administrators who share an administrative or System password shall keep the password stored securely.

5.5.2 **Changing Passwords** - System Administrators shall immediately change the password of their administrative or System account after the password or the administrative resource has been, or is suspected of being, compromised and when a System Administrator who shares this password separates from employment or changes jobs within King County. If this account is a System Account and a password change is not possible, the Organization shall perform a Risk Assessment and develop addition security measures and provide a copy to the county Chief Information Security and Privacy Officer.

5.6 **Training and Awareness** – Organizations shall provide Workforce Members annual training on this policy and their responsibilities for password management.

5.7 **Compliance** - Organizations shall include this policy in the annual compliance review as specified in the **Enterprise Information Security Policy**.

## 6.0 <u>EXCEPTIONS:</u>

Any Organization seeking an exception to this policy must follow the Information Technology Policy and Standards Exception Request Process using the Policy and Standards Request form. This form can be found on the Office of Information Resource Management policies and procedures Web page at http://kcweb.metrokc.gov/oirm/policies.aspx.

## 7.0 <u>RESPONSIBILITIES:</u>

7.1 **Workforce Members** comply with this policy, follow its guidelines, and understand the ramifications of all activities involving his/her Authentication Credentials.

7.2 **System Administrators** maintain the integrity of Workforce Member passwords and passwords for administrative resources, comply with this policy, and follow its guidelines.

7.3 **Organization Management** advise System Administrators when a Workforce Member no longer needs access to a System (such as, upon termination or job

change), provide training to Workforce Members reinforcing good password management practices, and  require compliance with this policy.